UNDER ATTACK

Another computer system break-in. Statistics show more will come. Almost 70 percent of commercial DPE/MIS organizations reported some form of information security incident in 1997. Computer data theft can result in huge money losses as computer crackers gain unauthorized access to a government agency or company's business through the Internet.

In the past, attackers have been mainly hobbyists with too much time on their hands. They are more satisfied by just taking on the sheer challenge of a computer system break-in. But attacks today have become malicious, intent on damage and piracy of intellectual property. A warning from the U.S. Department of Justice underscores the fact that the number of cyberspace criminals on the Internet will exceed five million by the year 2000.

Information security experts at Diversified High Technologies, Inc. (DHT) of Houston, Texas support the Johnson Space Center (JSC), providing information systems security safeguards.

DHT's mission statement is blunt: "Help organizations enhance productivity and protect their facilities and assets by business technologies integration without impacting ongoing operations."

In response to a 1992 NASA-wide cost saving directive, JSC's Engineering Directorate established the Avionics Software Development Environment Pathfinder (ASDEP) program. This activity evaluated Internet security technologies for mission critical facilities.

DHT experts in security systems are ready to help foil cyberspace break-in, an ever-growing security threat to businesses that rely on the Internet.

DHT has supported JSC's ASDEP program throughout its phases. For the first two years, DHT operated as the technology facilitator, providing technical coordination between vendors, contractors, and NASA. As technology facilitator, DHT helped coordinate the requirements and implementation of then state-of-the-art firewall functions such as dynamic network address translation (NAT) and encrypted private virtual networks (PVNs). DHT has recently provided support in secure technology migration path planning and the incorporation of new security technologies in response to JSC's evolving program needs.

JSC's ASDEP is now operating six "firewall" systems nationwide. A firewall is a set of components placed between two networks that collectively have these elements: all traffic from inside to outside and outside to inside must pass through the firewall; only authorized traffic, as defined by a business or government agency, will be allowed to pass; and the firewall itself is highly resistant to penetration.

The six firewall systems securely interconnect NASA and contractor facilities, using the Internet, to conduct mission critical functions for Space Shuttle onboard software development.

Knowledge gained by DHT in the NASA ASDEP program has allowed the company to successfully offer security services to the commercial marketplace. DHT has developed and is offering to both the commercial and government marketplaces, advanced information systems security services. These systems include: single sign-on, distributive computing environments, network intrusion detection, and independent security verification and certification.

The firm has developed a comprehensive information systems security program. Staying abreast of the leading edge information systems security technologies, new concepts are brought forward for customer consideration.

One of many valuable aids put to use by DHT is the technology test bed. The test bed, a subnet with a firewall system, is used to evaluate network security and connectivity technologies. That evaluation helps determine what major products are required and the corresponding integration needs. This test bed concept was directly derived from ASDEP.

DHT's goal in working with its customers is simple and direct: "To minimize the customer's Internet information security risks by providing a cost-effective, efficient, and well-implemented information systems security solution."